

ネットワーク技術の教科書

長谷和幸 [著]

一歩進んだ知識があなたの武器になる！

実務にも、試験対策にも、
両方に役立つ万能書！

第 1 章 ネットワークの基礎知識

1.1	伝送・交換方式	8
1.1.1	同期方式	8
1.1.2	アナログ伝送とデジタル伝送	11
1.1.3	変調方式	13
1.1.4	通信方式と回線の関係	17
1.1.5	多重化方式	21
1.1.6	交換方式	24
1.2	通信プロトコルの体系化	27
1.2.1	OSI の基本概念	27
1.2.2	OSI 基本参照モデル	29
1.2.3	OSI と TCP/IP	32
1.2.4	端末インタフェース	37
1.2.5	HDLC 手順	39
1.2.6	誤り検出・訂正方式	42
1.2.7	これまでの主な WAN サービス	45
1.3	回線に関する計算	49
1.3.1	データ転送時間	49
1.3.2	ビット誤り率	50
1.3.3	トラフィック計算	51
1.3.4	待ち行列計算	54
1.3.5	信頼度計算	59
1.4	演習問題	63

第 2 章 LAN の方式

2.1	LAN のトポロジ	68
2.2	CSMA/CD 方式 (IEEE 802.3)	71
2.3	無線 LAN (IEEE 802.11)	90
2.4	無線 LAN のセキュリティ	100
2.4.1	アクセスポイントへの不正接続対策	100
2.4.2	WEP	100
2.4.3	IEEE 802.11i	102
2.4.4	WPA	103
2.4.5	WPA2	105
2.5	無線 PAN (IEEE 802.15)	109
2.6	その他の LAN 関連技術	111
2.6.1	トークンパッシング方式	111
2.6.2	FDDI	113
2.6.3	PLC	113
2.7	演習問題	115

第3章 IP

3.1	パケットフォーマット	120
3.2	IPv4 アドレス	125
3.3	ルーティングテーブル (経路表)	133
3.4	アドレス変換	139
3.5	ICMP	147
3.6	IP マルチキャスト	152
3.7	DHCP	157
3.8	VRRP	162
3.9	モバイル IP	166
3.10	IPv6	169
3.11	IPv6/IPv4 共存技術	180
3.12	演習問題	187

第4章 TCPとUDP

4.1	TCP セグメント	192
4.2	TCP の通信方式	197
4.3	UDP データグラム	201
4.4	演習問題	203

第5章 アプリケーションプロトコル

5.1	HTTP とクッキー	206
5.1.1	HTTP	206
5.1.2	クッキー	213
5.1.3	HTTP 関連プロトコル	219
5.2	FTP	222
5.3	SNMP	227
5.4	NAS と SAN	232
5.5	CoAP	238
5.6	その他のプロトコル	240
5.7	演習問題	242

第6章 DNSの仕組み

6.1	ドメイン名の構成	246
6.2	資源レコード	250
6.3	DNS サーバの種類とキャッシュ	259
6.4	DNS プロトコル	262
6.5	DNS のセキュリティ	267
6.6	演習問題	273

第7章 電子メールの仕組み

7.1 電子メールの配送	276
7.2 電子メールのメッセージ構成	278
7.3 SMTP	283
7.4 POPとIMAP	287
7.5 電子メールのセキュリティ	292
7.5.1 電子メールの不正中継とその対策	292
7.5.2 送信ドメイン認証	296
7.5.3 その他のセキュリティ対策	302
7.6 演習問題	306

第8章 VoIP

8.1 SIP	310
8.2 RTP	319
8.3 演習問題	324

第9章 ネットワーク機器

9.1 LAN 間接続装置	326
9.2 ルーティングプロトコル	334
9.2.1 RIP	334
9.2.2 OSPF	337
9.2.3 BGP-4	342
9.2.4 TRILL	360
9.3 LAN スイッチ	353
9.3.1 レイヤ2スイッチとその機能	353
9.3.2 VLAN (バーチャル LAN)	357
9.3.3 経路制御	365
9.3.4 レイヤ3スイッチ	371
9.3.5 仮想スイッチ	376
9.4 ネットワーク仮想化	381
9.4.1 オーバーレイ方式	381
9.4.2 ホップバイホップ方式	384
9.5 演習問題	386

第10章 インターネット関連技術

10.1 ブロードバンド回線	392
10.1.1 ADSL	392
10.1.2 FTTH	393
10.1.3 CATV インターネット	395
10.2 PPPとPPPoE	397

10.2.1	PPP	397
10.2.2	PPPoE	402
10.3	マルチホーミング	405
10.4	ファイアウォールとIDS	409
10.4.1	ファイアウォール	409
10.4.2	IDSとIPS	415
10.5	演習問題	419

第11章 ネットワークセキュリティ

11.1	ネットワーク利用時におけるリスク	422
11.2	暗号化技術	432
11.3	認証技術	441
11.3.1	デジタル署名	441
11.3.2	ワンタイムパスワード	443
11.3.3	CA	445
11.3.4	時刻認証	451
11.3.5	メッセージ認証	452
11.4	レイヤ2トンネリングプロトコル	455
11.4.1	PPTP	455
11.4.2	L2TP	457
11.5	IPsec	459
11.5.1	AH	459
11.5.2	ESP	461
11.5.3	IPComp	466
11.5.4	IKE	466
11.6	TLS	473
11.7	Diffie-Hellmanの鍵交換方式	482
11.8	認証プロトコル	485
11.8.1	IEEE 802.1X	485
11.8.2	RADIUS	489
11.8.3	SAML	492
11.9	演習問題	494

演習問題の解答・解説	499
------------	-----

用語 INDEX	540
----------	-----

商標表示

各社の登録商標及び商標、製品名に対しては、特に注記のない場合でも、これを十分に尊重いたします。

第 1 章

ネットワークの基礎知識

1.1 伝送・交換方式	8
1.2 通信プロトコルの体系化	27
1.3 回線に関する計算	49
1.4 演習問題	63

1.1 伝送・交換方式

1.1.1 同期方式

▶同期

▶ビット同期

▶ブロック同期

データ伝送では“0”と“1”の情報しか送信しないため、受信側では送信データの先頭ビットが分からず、どのビットから検出すべきかが不明となる。そこで、送信側と受信側でタイミングを合わせて、送信されてきた信号からビットを正確に取り出す操作が必要となる。このような操作のことを**同期**という。

この同期には、ビットごとにタイミングを合わせる**ビット同期**と、各符号の先頭位置を知るために符号を示すビット列を一つの単位としてタイミングをとる**ブロック同期**の二つがある。なお、ブロック同期は、データリンク層のデータを取り出す操作に当たるので、同期制御と呼ばれることもある。

FAQ

Q：同期は、なぜ必要になるのでしょうか。

A：人間対人間による電話の場合について、最初に考えてみましょう。電話機の番号を押し、呼出し音が鳴った後、相手が応答すると、「もし、もし」などといって相手が誰であるかを確認して用件などを話し始めます。この「もし、もし」が会話を始める合図になっており、これがいわゆる同期に相当するものです。

では、機械対機械の通信を考えてみましょう。機械対機械の通信では、送信側から送る情報は、基本的に0,1の情報だけです。受信側は、情報がいつ来てもいいように準備していますが、伝送途中で0,1の信号が劣化したりすると、送られてきた先頭のビット位置が不明になってしまいます。そこで、受信側で先頭の位置を正しく検出できるように送信側が情報を送る際には、様々な工夫を採り入れて、情報を送るようにしています。様々な工夫があるがゆえに、同期方式を理解することを難しくさせていますが、データ通信においては、送信側と受信側が同期して情報を扱えるようにすることが、最も基本的かつ重要なことなのです。

(1) ビット同期

ビット同期には、送信側の同期信号とは関係なく送信側のタイミングでデータの先頭に、そのデータの始めを示すビットを付けてビット位置を知らせる**非同期**

▶非同期

▶ 連続同期

方式と、データとは別に常に同期信号を送りビット位置を知らせる**連続同期**方式の二つがある。

(a) 非同期方式

非同期方式は、受信側とは無関係に送信側のタイミングで送信するものである。調歩同期方式、あるいはスタートストップ同期方式ともいう。ベーシック伝送制御手順で採用されていた方式である。

▶ 調歩同期

調歩同期方式とは、ビット同期をとるため、各文字データ（例えば、8ビット）の前後に、スタートビットとストップビットを付けて伝送する方式をいう。例えば、スタートビットを“0”，ストップビットを“1”と決めておき、データを送る前の状態では常にストップビットの“1”を送っている。そこで、文字データの伝送が始まると、スタートビットの“0”が送り出される。この1→0の変化を受信側では常時監視しており、この変化を識別すると、文字データが送られてきたと認識する。そして、スタートビットの次のビットから順に読み取り、8ビットを読み取った後、次のビットがストップビットであることを確認して1文字分の読み取りを終了する。

調歩同期方式では、1文字が8ビットのデータを送る場合、スタートビットとストップビットの2ビットが付加されるため、合計10ビットが必要となり、伝送効率は少なくとも20%は低下することになる。

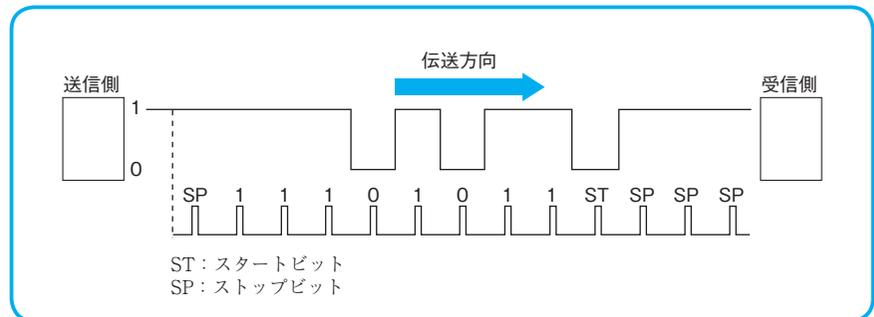


図 1-1 調歩同期方式

▶ 同期方式

(b) 連続同期方式

連続同期方式（**同期方式**ともいう）は、データとは別に常に同期信号を送りビット位置を知らせる方式である。このため、当初はデータを送る信号線と、同期信号を送る信号線の2本の線を設けて信号を送る方法を採用していたが、回線コストがかかり、現在では基本的に使われていない。そこで、LANにおけるマンチェスタ符号方式のように、1本の通信回線上にデータと同期信号（クロック情報）を重ね合わせて送り出す方法が、一般的に採用されている。なお、受信側では、同期信号を基にしてデータを取り出す。

同期方式では、ビットごとに同期がとれるので、一度に長いデータを送ることができる。また、同期用の特別なビットを付ける必要がないので、伝送効率や伝

送速度を向上させることができる。したがって、ビット同期においては、ほとんどが連続同期方式を採用している。

(2) ブロック同期

ビット同期によって各ビットが正しく識別できても、そのビット列のどこからどこまでが、一つの文字に対応しているかが分からなければ、ビット列を文字に変換することはできない。そこで、文字又はブロックの先頭位置を知るが必要になる。この方法としては、キャラクタ同期方式、フラグ同期方式などがある。なお、調歩同期方式では、スタートビットによって文字の先頭位置を検出できるので、ビット同期とブロック同期が同時に行われていることになる。

(a) キャラクタ同期方式

キャラクタ同期方式では、図 1-2 に示すように、同期をとるための特別なビットパターンをデータの前に付けて送り出す。ベーシック伝送制御手順では、“00010110”（低位のビットから順に送る）というパターンが使われる。これが SYN 符号である。SYN 符号は同期を確実にとるため、通常、二つ以上続けて送られる。

▶ キャラクタ同期

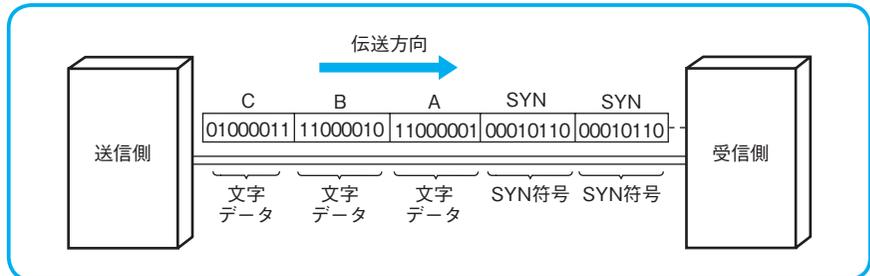


図 1-2 キャラクタ同期方式

受信側では、この SYN 符号を監視することによって同期をとる。同期がとれた後は 8 ビットずつ順番に取り出して 1 文字とみなし、文字を組み立てる操作を行う。

調歩同期方式では、1 文字ずつ同期をとっていたが、キャラクタ同期方式では、連続して送られてくる文字を受信することができる。文字と文字の間が時間的に空くことはなく、効率の良い伝送ができることから、導入された方式である。

(b) フラグ同期方式

フラグ同期方式は、あらかじめ決められた同期用のビットパターンを送信データの始めと終わりに付けて送り出す方式である。**フレーム同期**方式とも呼ぶ。

HDLC 手順では、特別なビット列“01111110”をデータの前後に付けて相手に送り出す。この特別なビット列を**フラグ**と呼んでおり、このフラグで囲まれた部分を、受信側では受信データとみなす。また、データがないときでもフラグは

▶ フラグ同期

▶ フレーム同期

▶ HDLC : High-level Data Link Control

▶ フラグ

1.4 演習問題

問 1-1

■ H27 秋 NW 午前Ⅱ問 3

OSI 基本参照モデルのトランスポート層の機能として、適切なものはどれか。

- ア 経路選択機能や中継機能を持ち、透過的なデータ転送を行う。
- イ 情報をフレーム化し、伝送誤りを検出するためのビット列を付加する。
- ウ 伝送をつかさどる各種通信網の品質の差を補完し、透過的なデータ転送を行う。
- エ ルータにおいてパケット中継処理を行う。

問 1-2

■ H27 秋 NW 午前Ⅱ問 6

HDLC 手順で用いられるフレーム中のフラグシーケンスの役割として、適切なものはどれか。

- ア 受信確認を待たずに複数フレームの送信を可能にする。
- イ フレームの開始と終了を示す。
- ウ フレームの転送順序を制御する。
- エ フレームの伝送誤りを検出する。

問 1-3

■ H24 秋 NW 午前Ⅱ問 8

ハミング符号の用途の説明として、適切なものはどれか。

- ア Bluetooth 通信で、ビット誤りを訂正するために使われている。
- イ G3 ファクシミリで画像データの圧縮に使われている。
- ウ HDLC フレーム内のビット誤りを検出するために使われている。
- エ MP3 でオーディオデータの圧縮に使われている。

第1章 ネットワークの基礎知識

問 1-1 ウ

OSI トラnsポート層の機能 ■ H27 秋 NW 午前 II 問 3

OSI 基本参照モデルのトラnsポート層（第4層）は、伝送をつかさどる各種通信網の品質の差を補完し、透過的なデータ転送を行う機能を提供する層である。したがって、（ウ）が正しい。

その他の記述は、次の各層の役割である。

ア：「経路選択機能や中継機能をもち」という記述から、ネットワーク層（第3層）になる。

イ：「伝送誤りを検出するためのビット列を付加する」という記述から、データリンク層（第2層）になる。

エ：「ルータにおいてパケット中継処理を行う」という記述から、ネットワーク層（第3層）になる。

問 1-2 イ

HDLC 手順のフラグシーケンス ■ H27 秋 NW 午前 II 問 6

HDLC（High-level Data Link Control：ハイレベルデータリンク制御）手順で用いられるフラグシーケンスは、“01111110”というビットパターンをもち、フレーム間の同期を取ったり、フレームの開始と終了を示したりするために使用される。したがって、（イ）が正しい。

その他の記述が示すものは、次のとおりである。

ア：HDLC フレームの連続転送に関する記述であり、最大7フレームまで送信することができる。これは、制御部にあるシーケンス番号の役割である。

ウ：HDLC フレームの転送順序の制御も、制御部にあるシーケンス番号の役割である。

エ：HDLC フレームのFCS（Frame Check Sequence）の役割である。

問 1-3 ア

ハミング符号の用途 ■ H24 秋 NW 午前 II 問 8

ハミング符号とは、情報ビットに対し誤り訂正用の冗長ビット（ECC：Error Correcting Code）を付加して、ビット誤りが生じてもその誤りを自動的に訂正する符号化方式のことをいう。データ通信だけでなく、メモリに情報を記録する際などにも利用されている。例えば、無線LANのBluetoothでは、S/N比の低下や電波干渉などによって情報誤りが発生するので、情報10ビットに対し、ECCを5ビット付加してビット誤りを訂正するようにしている。したがって、（ア）が正しい。

その他の記述が示すものは、次のとおりである。

イ：MR（Modified READ）と呼ばれる符号化方式

ウ：FCS（Frame Check Sequence）

エ：MPEG-1における音声のレイヤ3というデータ圧縮方式（MP3）

問 1-4 ウ

最大論理回線数の算出 ■ H28 秋 NW 午前 II 問 3

X地点からY地点まで同時に使用できる論理回線数を求めるためには、次の図のように（1）～（4）の各断面における多重度を計算していくとよい。すると、（1）が11、（2）が10、（3）が11、（4）が12となる。

用語 INDEX

<数字・記号>

\$INCLUDE	257
\$ORIGIN	256
\$TTL	257
@	257
10BASE-T	73
10GBASE-T	68
100BASE-TX	73
1000BASE-T	73
2線式	20
3ウェイハンドシェイク	197
4B/5B	77
4B/5B変換	113
4D-PAM5	78
4線式	20
4バイトAS番号	349
6to4	182
6to4対応ホスト	182
8B1Q4	78

< A >

ABR	342
ACE	248
ACK	194, 311
ADPCM	16
ADSL	392
ADSLモデム	37, 393
AES	436
AH	459
APN	331
APNIC	125
APOP	294
ARP	35, 130
ARPANET	32
ARPキャッシュ	130
ARPテーブル	130

ARQ	42
AS	342
AS_PATH属性	346
ATM	47
AUI	72
AUIケーブル	73
Automatic MDI/MDI-X	354
AAAAレコード	254
Aレコード	254

< B >

B-PON	402
B-TAG	363
B2BuA	318
BAS	402
Bcc	281
BGP-4	343, 407
BGP4+	180
BGPスピーカ	343
BGPピア	344
BIND	257
BOOTP	157
BPDU	365
BPSK	92
BSS	91
BSSID	91
BYE	311

< C >

C-TAG	363
CA	445
CATV	395
CATVインターネット	396
CA証明書	447, 477
CBC	106
Cc	281

CCK	92
CCMP	105
CDM	24
CDMA	24
CEルータ	375
CGN	144
CHAP	400
CIDR	128
CIFS	232
CN	448
CNAMEレコード	254
CoAP	238
CODEC	16
Connection	210
Cookie	211
CoS	360
CRC方式	42
CRL	449
CRLF	284, 310
CRYPTREC	439
CS-ACELP	17
CSMA/CA	94
CSMA/CA + ACK	95
CSMA/CD	71
CSR	450

< D >

DAD	175
DAS	232
DATAコマンド	284
DCE	37
DDoS攻撃	426
DES	435
DFS	99
DHCP	157
DHCPACK	160